Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1–3. (Cancelled)

4. (Currently Amended) A method of verifying knowledge of a secret number s in a prover device by a verifier device having no knowledge of the secret number, the method comprising a zero-knowledge protocol using a Montgomery representation of numbers and Montgomery multiplication operations therein,

wherein the zero knowledge protocol comprises the Fiat-Shamir protocol,

~~The method of claim 2 including the steps of:~~

the method further comprising:

(i) providing to the verifier device a value $v = s^2$ being the Montgomery multiplication of the secret number s by itself,

(ii) computing, by the prover device, [[the]] a value $x = r\ x_m\ r$, where r is a random number, and transmitting the value [[of]] x to the verifier device;

(iii) selecting, by the verifier device, a challenge value of e from [[the]] a set {0, 1} and transmitting the challenge value to the prover device;

(iv) computing, by the prover device, [[the]] a value $y = r\ x_m\ s^e$, and transmitting the value y to the verifier device; and

(v) the verifier device checking [[the]] an authenticity of the prover's response according to the values [[of]] x, y and v previously received and according to the challenge value e.

5. (Previously Presented) The method of claim 4 wherein the step of checking the authenticity of the prover's response comprises the steps of:

for a challenge value of e = 1, computing the values of $y\ x_m y$ and $v\ x_m x$ and checking that they are the same; or

for a challenge value of e = 0, computing the value of $y\ x_m y$ and checking that it is the same as the previously received value of x.

6. (Currently Amended) The method of claim 4 further including the steps of repeating steps (ii) to (v) for a number of consecutive rounds to confirm the authenticity of the prover's response [[device.]]

7. (Previously Presented) The method of claim 4 in which the secret number s is a Montgomery representation of another number s' known in the prover device domain but not in the verifier device domain, further including the step of computing, by the prover device, the value of s from s' according to s = s'R mod n, where R>n, values of n and R being used by both the prover device and the verifier device.

8. (Previously Presented) The method of claim 4 in which the Montgomery multiplications of $s\ x_m s$, $r\ x_m\ r$, and $r\ x_m\ s^e$ are carried out according to the formula $a\ x_m b=abR^{-1}\text{mod } n$, where R>n, values of n and R being used by both the prover device and the verifier device.

9. (Previously Presented) The method of claim 5 in which the Montgomery multiplications of $y\ x_m y$ and $s^2\ x_m x$ are carried out according to the formula $a\ x_m b = abR^{-1}\text{mod } n$, where R>n, values of n and R being used by both the prover device and the verifier device

10. (Currently Amended) The method of claim [[1]] 4 in which all computations in the zero knowledge protocol are performed using Montgomery representation of numbers and using Montgomery multiplication operations.

11. (Currently Amended) A method of verifying knowledge of a secret number s in a prover device by a verifier device having no knowledge of the secret number, the method

comprising a zero-knowledge protocol using a Montgomery representation of numbers and Montgomery multiplication operations therein,

~~The method of claim 3 including the steps of:~~

wherein the zero knowledge protocol comprises the Guillou-Quisquater protocol,

the method further comprising:

(i) providing to the verifier device a value s^e being [[the]] a Montgomery e^{th} power of the secret number s;

(ii) computing, by the prover device, [[the]] a value $x = r^e$, being [[the]] a Montgomery e^{th} power of r, where r is a random number, and transmitting the value of x to the verifier device;

(iii) selecting, by the verifier device, a challenge value [[of]] c from [[the]] a set {0, 1, ... e-1} and transmitting the challenge value c to the prover device;

(iv) computing, by the prover device, [[the]] a value $y = r\, x_m\, s^c$ and transmitting the value y to the verifier device; and

(v) ~~the verifier device~~ checking, by the verifier device, the authenticity of the prover's response according to the values [[of]] x, y and s^e previously received and according to the challenge value c.

12. (Currently Amended) The method of claim 11 wherein ~~the step of~~ checking the authenticity of the prover's response comprises~~the step of~~:

computing the values of y^e and $x\, x_m\, s^{ec}$ and checking that they are the same.

13. (Currently Amended) The method of claim 11 further comprising ~~including the steps of~~repeating steps (ii) to (v) for a number of consecutive rounds to confirm the authenticity of the prover's response. [[device.]]

14. (Cancelled)

15. (Currently Amended) A prover device having contained therein a secret number s in Montgomery representation, the prover device adapted for proving knowledge of the secret

number s to a verifier device without conveying the knowledge of the secret number itself, with a zero-knowledge protocol using the Montgomery representation of numbers and Montgomery multiplication operations therein, comprising: ~~The prover device of claim 14 further including:~~

means for selecting a random number, r;

means for computing [[the]] a Montgomery ~~squareof~~ square of r to obtain x = r^2;

means for transmitting x to [[a]] the verifier device;

means for receiving a challenge value, e;

means for computing [[the]] a Montgomery product of y = r x_m s; and

means for transmitting y to the verifier device.

16. (Currently Amended) A prover device having contained therein a secret number s in Montgomery representation, the prover device adapted for proving knowledge of the secret number s to a verifier device without conveying the knowledge of the secret number itself, with a zero-knowledge protocol using the Montgomery representation of numbers and Montgomery multiplication operations therein, comprising: ~~The prover device of claim 14 further including:~~

means for selecting a random number, r;

means for computing [[the]] a Montgomery e^{th} power of r to obtain x = r^e;

means for transmitting x to [[a]] the verifier device;

means for receiving a challenge value, c;

means for computing [[the]] a Montgomery product of y = r x_m s; and

means for transmitting y to the verifier device.

17. (Cancelled)

18. (Currently Amended) A verifier device for verifying knowledge of a secret number s in a prover device without knowledge of the secret number itself, wherein the verifier device is adapted to utilize a zero-knowledge protocol using the Montgomery representation of numbers and Montgomery multiplication operations therein, comprising: ~~The verifier device of claim 17 further including:~~

means for receiving [[the]] a Montgomery square v of the secret number s;

means for receiving [[the]] a Montgomery square[[,]] x of [[the]] a secret number[[,]] r;

means for transmitting a challenge value[[,]] e to the prover device;

means for checking [[the]] authenticity of ~~the prover's~~ a response[[,]] y from the prover device, according to [[the]] a Montgomery square of y verified against values of x and / or v received from the prover device according to the challenge value[[,]] e.

19. (Currently Amended) A verifier device for verifying knowledge of a secret number s in a prover device without knowledge of the secret number itself, wherein the verifier device is adapted to utilize a zero-knowledge protocol using the Montgomery representation of numbers and Montgomery multiplication operations therein, comprising: ~~The verifier device of claim 17 further including:~~

means for receiving [[the]] a Montgomery e^{th} power[[,]] s^e of the secret number s;

means for receiving [[the]] a Montgomery e^{th} power[[,]] x of a random number[[,]] r;

means for transmitting a challenge value[[,]] c to the prover device;

means for checking [[the]] authenticity of ~~the prover's~~ a response[[,]] y from the prover device, according to [[the]] a Montgomery e^{th} power of y verified against [[the]] a value of $x\ x_m\ s^{ec}$ received from the prover device[[,]] according to the challenge value[[,]] c.

20. (Currently Amended) A method of proving [[the]] knowledge of a secret number s in a prover device to a verifier device having no knowledge of the secret number s, [[with]] utilizing a zero-knowledge protocol using [[the]] a Montgomery representation of numbers and Montgomery multiplication operations therein, the method comprising~~ the steps of~~:

selecting a random number[[,]] r;

computing [[the]] a Montgomery e^{th} power of r to obtain x;

transmitting x to [[a]] the verifier device;

receiving a challenge value[[,]] c;

computing [[the]] a Montgomery product of $y = r\ x_m\ s^c$; and

transmitting y to the verifier device.

21. (Currently Amended) A method of verifying [[the]] knowledge of a secret number s in a prover device by a verifier device having no knowledge of the secret number s, [[with]] utilizing a zero-knowledge protocol using [[the]] a Montgomery representation of numbers and Montgomery multiplication operations therein, the method comprising~~ the steps of~~:

receiving [[the]] a Montgomery square v of the secret number s;

receiving [[the]] a Montgomery square[[,]] x of a random number[[,]] r;

transmitting a challenge value[[,]] e to the prover device;

checking [[the]] authenticity of ~~the prover's~~ a response[[,]] y from the prover device, according to [[the]] a Montgomery square of y verified against values of x and / or v received from the prover device according to the challenge value e.

22. (Currently Amended) A method of verifying [[the]] knowledge of a secret number s in a prover device by a verifier device having no knowledge of the secret number s, [[with]] utilizing a zero-knowledge protocol using [[the]] a Montgomery representation of numbers and Montgomery multiplication operations therein, the method comprising~~ the steps of~~:

receiving [[the]] a Montgomery e^{th} power of the secret number s;

receiving [[the]] a Montgomery e^{th} power[[,]] x of a random number[[,]] r;

transmitting a challenge value[[,]] c to the prover device;

checking [[the]] authenticity of ~~the prover's~~ a response[[,]] y from the prover device, according to [[the]] a Montgomery e^{th} power of y verified against [[the]] a value of $x\ x_m\ s^{ec}$ received from the prover device according to the challenge value c.

23–26. (Cancelled)

27. (New) The method of claim 4, further comprising a computer program product comprising a computer readable medium having thereon computer program code means adapted, when said program is loaded onto a computer, to make the computer execute the method.

28. (New) The method of claim 4, further comprising a computer program, distributable by electronic data transmission, comprising computer program code means adapted, when said program is loaded onto a computer, to make the computer execute the method.

29. (New) The method of claim 11, further comprising a computer readable medium having thereon computer program code means adapted, when said program is loaded onto a computer, to make the computer execute the method.

30. (New) The method of claim 11, further comprising a computer program, distributable by electronic data transmission, comprising computer program code means adapted, when said program is loaded onto a computer, to make the computer execute the method.